كتاب إلكتروني

الحماية
شديد الأهمية
بنية تحتية



segura®

مقدمة

ضرورة تأمين الأمور الحيوية
البنية التحتية في المشهد الرقمي الحالي

في عالمنا المترابط اليوم، تُشكل البنية التحتية الحيوية العمود الفقري لمجتمعنا، إذ تُمكّن من توفير خدمات أساسية كقطاعات الطاقة والنقل والرعاية الصحية والاتصالات. ومع ذلك، بات تأمين هذه الأنظمة الحيوية أكثر صعوبةً مع استمرار تطور التهديدات السيبرانية وازدياد تعقيدها. وبعد أن ذكرت وكالة الأمن السيبراني للاتحاد الأوروبي (ENISA)أن 30%من جميع الهجمات السيبرانية استهدفت قطاعات البنية التحتية الحيوية في عام 2019، أصبحت الحاجة إلى تدابير أمنية قوية أكثر إلحاحًا من أي وقت مضى.

قد تكون عواقب الاختراقات الأمنية في البنية التحتية الحيوية وخيمة. إذ تواجه المؤسسات خسائر مالية فادحة، حيث يُقدّر معهد بونيمون متوسط تكلفة اختراق البيانات لمؤسسات البنية التحتية الحيوية بنحو 4.29مليون دولار. إضافةً إلى ذلك، قد يكون لانقطاع الخدمات الأساسية آثار اجتماعية واقتصادية واسعة النطاق. يُذكر أن 85%من البنية التحتية الحيوية في الولايات المتحدة مملوكة ومدارة من قبل القطاع الخاص.

يُبرز تقرير الجمعية الأمريكية للمهندسين المدنيين (ASCE)لعام 2021حول البنية التحتية الحاجة إلى استثمارات كبيرة لتحسين وتأمين البنية التحتية الحيوية للبلاد، مما منح الولايات المتحدة تقديرًا متدنيًا (-C).ومع تقديرات وكالة الطاقة الدولية (IEA)بأن الاستثمارات العالمية في البنية التحتية للطاقة يجب أن تصل إلى 3.5تريليون دولار سنويًا حتى عام 2050لتحقيق أهداف المناخ والطاقة العالمية، تزداد أهمية تأمين هذه الاستثمارات.

في هذا الكتاب الإلكتروني، سنستكشف أهمية البنية التحتية الحيوية، والتهديدات والتحديات المختلفة التي تواجهها، ودور إدارة الوصول المتميز (PAM)في ضمان أمنها. كما سنقدم حل Segura® PAMونوضح كيف يمكنه حماية أنظمة البنية التحتية الحيوية بفعالية في بيئة رقمية سريعة التطور.

من خلال فهم المخاطر وتطبيق تدابير أمنية قوية، يمكن للمؤسسات حماية بنيتها التحتية الحيوية وضمان استمرار تقديم الخدمات الأساسية لسنوات قادمة.

جدول المحتويات



كتاب إلكتروني

حماية البنية التحتية الحيوية

الفصل الأول

مقدمة في النقد

البنية التحتية وأهميتها

تعريف
شديد الأهمية
بنية تحتية

مع ازدياد ترابط العالم، بات تأمين واستقرار البنية التحتية الحيوية أمراً لا غنى عنه لحسن سير المجتمع والاقتصاد. تشمل البنية التحتية الحيوية الأصول والأنظمة والشبكات، المادية منها والافتراضية، التي تُعدّ أساسية لعمليات الدولة. ويشمل ذلك قطاعات مثل الطاقة والمياه والنقل والاتصالات وخدمات الطوارئ، وغيرها.

قد يؤدي تعطيل أو تدمير هذه البنى التحتية الحيوية إلى عواقب وخيمة، لا تؤثر فقط على قطاعات محددة، بل تمتد لتشمل السلامة العامة والأمن القومي والاقتصاد ككل. ونتيجة لذلك، برزت أولوية أمن ومرونة البنية التحتية الحيوية كأحد الشواغل الرئيسية للحكومات والمنظمات في جميع أنحاء العالم.

أصبح استقرار البنية التحتية الحيوية أمراً لا غنى عنه لحسن سير عمل المجتمع والاقتصاد.

أهمية النقد

بنية تحتية

تُشكّل البنية التحتية الحيوية العمود الفقري للمجتمع الحديث، إذ تُوفّر خدمات أساسية تُؤثّر على جميع جوانب الحياة اليومية. ولا يُمكن المُبالغة في أهمية هذه البنية، فهي تضمن سلاسة عمل مختلف القطاعات.

قد يؤدي تعطل أو انقطاع أي من هذه البنى التحتية الحيوية إلى عواقب وخيمة، تشمل خسائر في الأرواح، وأضرارًا اقتصادية، وتآكلًا في ثقة الجمهور.

ولذلك، فإن حماية البنى التحتية الحيوية أمر بالغ الأهمية للحفاظ على الأمن القومي، والسلامة العامة، والاستقرار الاقتصادي.

الطاقة: توليد ونقل وتوزيع الكهرباء والغاز الطبيعي وأشكال الطاقة الأخرى التي تُشغل منازلنا وشركاتنا وصناعاتنا.

ماء

توفير مياه شرب نظيفة وآمنة، بالإضافة إلى معالجة مياه الصرف الصحي والتخلص منها.

النقل: حركة الأشخاص والبضائع جواً وبراً وبحراً، بما في ذلك الطرق السريعة والسكك الحديدية والموانئ والمطارات.

الاتصالات

نقل المعلومات عبر وسائط مختلفة، مثل الإنترنت وشبكات الهاتف وأنظمة الأقمار الصناعية.

خدمات الطوارئ: توفير الخدمات الطبية والشرطية وخدمات الإطفاء التي تحمي صحة وسلامة المواطنين.

النمو
الحاجة إلى أمر بالغ الأهمية
بنية تحتية
حماية

مع ازدياد ترابط العالم واعتماده على التكنولوجيا، تزايدت احتمالية الهجمات الإلكترونية على البنية التحتية الحيوية بشكل كبير. يستهدف مجرمو الإنترنت والدول والجهات الخبيثة الأخرى البنية التحتية الحيوية بشكل متزايد، ساعين إلى استغلال الثغرات الأمنية والوصول غير المصرح به إلى المعلومات الحساسة وأنظمة التحكم وغيرها من الأصول الحيوية.

وتتفاقم المخاطر المرتبطة بالتهديدات الإلكترونية للبنية التحتية الحيوية بسبب عوامل مثل:

• زيادة استخدام التقنيات الرقمية و تقارب أنظمة تكنولوجيا المعلومات (IT) وتكنولوجيا التشغيل (OT)، مما يخلق نقاط ضعف جديدة وأسطح هجوم.

• الاعتماد المتزايد على البائعين الخارجيين وشركاء سلسلة التوريد، مما قد يؤدي إلى مخاطر وتعقيدات إضافية.

• الوتيرة السريعة للتغير التكنولوجي، والتي يمكن أن تجعل من الصعب على المؤسسات مواكبة التهديدات المتطورة والحفاظ على وضع أمني قوي.

في ضوء هذه التحديات، أصبح من الأهمية بمكان أن تقوم المؤسسات بتنفيذ تدابير أمنية شاملة لحماية بنيتها التحتية الحيوية وضمان استمرار مرونتها.

دور المتميزين إدارة الوصول في ألبنية التحتية الحيوية حماية

يُعدّ التحكم الفعال في الوصول المتميز أحد المكونات الرئيسية لحماية البنية التحتية الحيوية.

يشير الوصول المميز إلى الأذونات المرتفعة الممنوحة لمستخدمين محددين، مما يسمح لهم بأداء مهام حساسة، أو الوصول إلى أنظمة حيوية، أو إدارة ضوابط الأمان.

تُعدّ إدارة الوصول المتميز (PAM)جانبًا بالغ الأهمية في أمن البنية التحتية الحيوية، إذ تُساعد المؤسسات على منع الوصول غير المصرح به، واكتشاف التهديدات والاستجابة لها، والامتثال لمعايير ولوائح الصناعة ذات الصلة. توفر حلول إدارة الوصول المتميز، مثل Segura® PAM، الأدوات والقدرات اللازمة لإدارة ومراقبة والتحكم في الوصول المتميز، مما يُقلل من مخاطر الاختراقات الأمنية ويحمي البنية التحتية الحيوية من الهجمات المحتملة.



في الفصول التالية، سنتعمق أكثر في التهديدات والتحديات التي تواجه أمن البنية التحتية الحيوية، ودور إدارة الوصول المتميز في مواجهة هذه التحديات، وكيف يعمل نظام ®Segura

يمكن أن يساعد حل إدارة الوصول المتميز (PAM)المؤسسات على حماية أصول البنية التحتية الحيوية.



كتاب إلكتروني

حماية البنية التحتية الحيوية

الفصل الثاني

التهديدات و

تحديات أمام النقد

بنية تحتية

حماية

فهم
مشهد التهديدات

تتعرض أمن البنية التحتية الحيوية لتهديد مستمر من جهات فاعلة متنوعة، تشمل الدول، ومجرمي الإنترنت، والناشطين الإلكترونيين، وحتى المتسللين من الداخل. تستخدم هذه الجهات الخبيثة أساليب وتقنيات وإجراءات مختلفة لاختراق أنظمة البنية التحتية الحيوية، وتعطيل الخدمات، أو إلحاق أضرار مادية بها. ومن أبرز التهديدات الشائعة لأمن البنية التحتية الحيوية ما يلي:

الهجمات الإلكترونية: يمكن لمجرمي الإنترنت والجهات الفاعلة التابعة للدول أنظمة البنية التحتية الحيوية باستخدام أنواع مختلفة من البرامج الضارة وبرامج الفدية والهجمات الحرمان من الخدمة الموزعة (DDoS) لتعطيل العمليات أو سرقة المعلومات الحساسة أو التسبب في أضرار مادية.

مصرح به للجهات الفاعلة المهددة.

المواد

يمكن أيضًا استهداف أصول البنية التحتية الحيوية بتهديدات مادية، مثل الإرهاب أو التخريب أو الكوارث الطبيعية، مما قد يتسبب في أضرار جسيمة أو تعطيل للعمليات.

التهديدات الداخلية

يمكن للموظفين أو المقاولين أو غيرهم من المطلعين الذين يتمتعون بصلاحيات وصول مميزة أن يعرقلوا أنظمة البنية التحتية الحيوية عن قصد أو عن غير قصد، سواء من خلال أعمال التخريب أو الإهمال.

التحديات في تأمين البنية التحتية الحيوية

تُعد حماية البنية التحتية الحيوية من التهديدات العديدة المذكورة أعلاه مهمة معقدة، وتزداد تعقيداً بسبب العديد من التحديات الفريدة، بما في ذلك:

•تقارب تكنولوجيا المعلومات وتكنولوجيا التشغيل: أدى دمج أنظمة تكنولوجيا المعلومات (IT)وتكنولوجيا التشغيل (OT)إلى زيادة الكفاءة والاتصال، ولكنه أدى أيضًا إلى ظهور ثغرات جديدة يمكن استغلالها من قبل مجرمي الإنترنت.

•الأنظمة القديمة: تعتمد العديد من قطاعات البنية التحتية الحيوية على أنظمة قديمة لم يتم تصميمها مع مراعاة التهديدات الأمنية الحديثة، مما يجعلها أكثر عرضة للهجمات.

•عدم كفاية الرؤية والمراقبة: الحجم الهائل
إن تعقيد أنظمة البنية التحتية الحيوية يجعل من الصعب على المؤسسات الحفاظ على رؤية كاملة ومراقبة لشبكاتها وأجهزتها ونقاط الوصول الخاصة بها.

•الامتثال التنظيمي: يجب على المنظمات المسؤولة عن البنية التحتية الحيوية الامتثال للوائح والمعايير المختلفة الخاصة بالصناعة، والتي يمكن أن تكون معقدة وتستغرق وقتًا طويلاً لإدارتها.

•موارد محدودة: العديد من البنى التحتية الحيوية
تواجه المنظمات قيودًا على الميزانية، ونقصًا في الموظفين، أو نقصًا في الخبرة الداخلية، مما يجعل من الصعب تنفيذ وصيانة تدابير أمنية قوية.

الدور الحاسم لـ الوصول المميز إدارة

نظراً للمخاطر والتحديات المرتبطة بأمن البنية التحتية الحيوية، فمن الضروري للمؤسسات تطبيق حل شامل لإدارة الوصول المتميز (PAM)، مثل Segura® PAM. يُعدّ PAM عنصراً أساسياً في أي وضع أمني قوي، حيث يساعد المؤسسات على:

يمكن لحلول إدارة الوصول المتميز (PAM) أن توفر مراقبة وتنبيهًا في الوقت الفعلي للأنشطة المشبوهة، مما يُمكّن المؤسسات من اكتشاف الحوادث الأمنية المحتملة والاستجابة لها بسرعة.

منع الوصول غير المصرح به

من خلال التحكم في الوصول المتميز وإدارته، يمكن للمؤسسات تقليل مخاطر الوصول غير المصرح به إلى الأنظمة الحيوية، سواء من المهاجمين الخارجيين أو من الداخلين.

يمكن أن توفر حلول إدارة الوصول المتميز (PAM) رؤية للمؤسسات المخترقة والتحكم الأمني في الوصول المتميز عبر بيئات تكنولوجيا المعلومات والتشغيل الخاصة بها، مما يقلل من مخاطر الاختراقات الأمنية.

تساعد حلول إدارة الوصول المتميز في الحفاظ على الامتثال التنظيمي المؤسسات على تلبية متطلبات اللوائح والمعايير الخاصة بالصناعة، مثل HIPAA وGDPR وNERC CIP، من خلال ضمان ضوابط الوصول المناسبة، والتدقيق، وقدرات إعداد التقارير.



في الفصل التالي، سنتناول دور إدارة الوصول المتميز بمزيد من التفصيل، بما في ذلك مكوناتها الرئيسية وكيف يمكنها مساعدة المؤسسات على حماية بنيتها التحتية الحيوية.

أصول.



الفصل الثالث

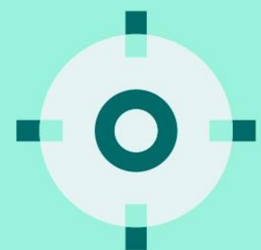
فهم دور ذوي الامتيازات

إدارة الوصول (PAM)

أهمية
الوصول المميز
إدارة

كما نوقش في الفصول السابقة، يعتمد أمن البنية التحتية الحيوية بشكل كبير على الإدارة والتحكم الفعالين في الوصول المتميز. يتمتع المستخدمون المتميزون، مثل مديري الأنظمة وموظفي تقنية المعلومات وموردي الطرف الثالث، بصلاحيات موسعة تمنحهم الوصول إلى الأنظمة الحيوية والمعلومات الحساسة.

إذا لم تتم إدارة هذا الوصول بشكل صحيح، فقد يتم استغلاله من قبل جهات خبيثة، مما يؤدي إلى اختراقات أمنية كبيرة وأضرار محتملة للبنية التحتية الحيوية.



تُعد إدارة الوصول المميز (PAM)عنصرًا أساسيًا في استراتيجية أمنية قوية، حيث تساعد المؤسسات على منع الوصول غير المصرح به، واكتشاف التهديدات والاستجابة لها، والحفاظ على الامتثال للوائح الخاصة بالصناعة.

المكونات الرئيسية لـ PAM

يتضمن حل إدارة الوصول المتميز الشامل، مثل Segura® PAM، عادةً المكونات الرئيسية التالية:

• التحكم في الوصول: توفر حلول إدارة الوصول المتميز (PAM) تحكمًا دقيقًا في الوصول تتيح الضوابط للمؤسسات تحديد وفرض صلاحيات الوصول إلى الأنظمة المختلفة، والشروط اللازمة لذلك، ومدة صلاحية الوصول. ويشمل ذلك ميزات مثل التحكم في الوصول القائم على الأدوار (RBAC)، والوصول الفوري (JIT)، والترقية المؤقتة للصلاحيات.

• إدارة بيانات الاعتماد: توفر حلول إدارة الوصول المتميز (PAM) إدارة مركزية لبيانات الاعتماد ذات الامتيازات، بما في ذلك كلمات المرور والمفاتيح والشهادات. ويشمل ذلك إمكانيات مثل التخزين الآمن والتدوير التلقائي والتدقيق الدوري لبيانات الاعتماد.

• مراقبة وتسجيل الجلسات: حلول إدارة الوصول المتميز (PAM) تُمكّن هذه التقنية المؤسسات من مراقبة وتسجيل جلسات المستخدمين ذوي الصلاحيات في الوقت الفعلي، مما يوفر رؤية شاملة ومساءلة كاملة عن الأنشطة التي تتطلب صلاحيات. ويساعد ذلك المؤسسات على اكتشاف الأنشطة المشبوهة ويسهل التحقيقات الجنائية الرقمية في حال وقوع حادث أمني.

• التدقيق وإعداد التقارير: توفر حلول إدارة الوصول المتميز (PAM) قدرات شاملة للتدقيق وإعداد التقارير، مما يسمح للمؤسسات بتتبع وتحليل أنشطة الوصول المميز وإثبات الامتثال للوائح والمعايير الخاصة بالصناعة.

• اكتشاف التهديدات والاستجابة لها: تتضمن حلول إدارة الوصول المتميز المتقدمة التعلم الآلي وتحليلات السلوك لتحديد الحالات الشاذة والتهديدات الأمنية المحتملة، مما يُمكّن المؤسسات من اكتشاف الحوادث والاستجابة لها بسرعة قبل تصاعدها.

فوائد التنفيذ PAMفي الحالات الحرجة بنية تحتية حماية

يوفر تطبيق حل قوي لإدارة الوصول المتميز (PAM)، مثل Segura® PAM، العديد من المزايا للمؤسسات المسؤولة عن البنية التحتية الحيوية، بما في ذلك:

أمان مُعزز

من خلال إدارة ومراقبة الوصول المتميز، يمكن للمؤسسات أن تقلل بشكل كبير من مخاطر الوصول غير المصرح به والاختراقات الأمنية، مما يحمي أنظمتها الحيوية ومعلوماتها الحساسة.

تساعد حلول إدارة الوصول المتميز (PAM) المحسّنة للامتثال المؤسسات على إثبات امتثالها لمختلف اللوائح والمعايير الخاصة بالصناعة من خلال توفير ضوابط الوصول اللازمة، والتدقيق، وقدرات إعداد التقارير.

زيادة الكفاءة التشغيلية من خلال أتمتة وتبسيط عمليات الوصول المتميز، يمكن لحلول إدارة الوصول المتميز (PAM) تحسين الكفاءة التشغيلية وتقليل مخاطر الخطأ البشري.

توفر حلول إدارة الوصول المتميز (PAM)للمؤسسات الرؤية والتحكم اللازمين لإدارة الوصول المتميز بشكل فعال عبر بيئات تكنولوجيا المعلومات والتشغيل الخاصة بها، مما يضمن منح الوصول المتميز فقط لأولئك الذين يحتاجون إليه حقًا.



سنتناول في الفصول التالية شركة سيغورا® PAMبمزيد من التفصيل، بما في ذلك ميزاته الرئيسية، وكيفية حمايته للبنية التحتية الحيوية، ودراسات حالة واقعية توضح فعاليته في العمل.



الفصل الرابع

سيجورا® بام:
نظرة عامة والميزات الرئيسية

مقدمة عن سيجورا® بام

Segura® Privileged Access Management (PAM) هو حل شامل مصمم لمساعدة المؤسسات على حماية بنيتها التحتية الحيوية من خلال إدارة والتحكم في الوصول المتميز عبر بيئات تكنولوجيا المعلومات والتشغيل الخاصة بها.

يوفر Segura® PAM مجموعة قوية من الميزات والقدرات التي تمكن المؤسسات من منع الوصول غير المصرح به، واكتشاف التهديدات والاستجابة لها، والحفاظ على الامتثال لمعايير ولوائح الصناعة ذات الصلة.

الميزات الرئيسية لـ Segura® PAM

يوفر Segura® PAM مجموعة واسعة من الميزات التي تجعله حلاً مثالياً للمؤسسات التي تسعى إلى تعزيز أمن بنيتها التحتية الحيوية. بعض الميزات الرئيسية لـ Segura®

تشمل PAM ما يلي:

• التحكم الدقيق في الوصول: يوفر نظام Segura® PAM التحكم في الوصول القائم على الأدوار (RBAC) والوصول الفوري (JIT)، مما يضمن حصول المستخدمين ذوي الصلاحيات على الوصول إلى الأنظمة التي يحتاجونها فقط عند الحاجة إليها. وهذا يساعد على تقليل مخاطر الوصول غير المصرح به والاختراقات الأمنية.

• إدارة بيانات الاعتماد الآمنة: يوفر Segura® PAM الإدارة المركزية لبيانات الاعتماد ذات الامتيازات، بما في ذلك كلمات المرور والمفاتيح والشهادات. ويشمل ذلك الأمان

التخزين والتدوير التلقائي والتدقيق الدوري لبيانات الاعتماد لضمان سلامتها وتقليل مخاطر الاختراق.

• مراقبة وتسجيل الجلسات: يُمكّن نظام Segura® PAM المؤسسات من مراقبة وتسجيل جلسات المستخدمين ذوي الصلاحيات في الوقت الفعلي، مما يوفر رؤية شاملة ومساءلة كاملة عن الأنشطة التي تتطلب صلاحيات. يساعد هذا في اكتشاف الأنشطة المشبوهة ويسهل التحقيقات الجنائية الرقمية في حال وقوع حادث أمني.

• الكشف المتقدم عن التهديدات والاستجابة لها: يدمج Segura® PAM التعلم الآلي والتحليلات السلوكية لتحديد الحالات الشاذة والتهديدات الأمنية المحتملة، مما يُمكّن المؤسسات من اكتشاف الحوادث والاستجابة لها بسرعة قبل تصاعدها.

• التدقيق وإعداد التقارير الشاملة: يوفر Segura® PAM إمكانيات تدقيق وإعداد تقارير شاملة، مما يسمح للمؤسسات بتتبع وتحليل أنشطة الوصول المميزة وإثبات الامتثال للوائح والمعايير الخاصة بالصناعة.

• التكامل مع البنية التحتية الحالية: يتكامل Segura® PAM بسلاسة مع أنظمة تكنولوجيا المعلومات وأنظمة التشغيل الحالية، مما يسهل على المؤسسات تنفيذ وإدارة سياسات الوصول المميزة الخاصة بها دون تعطيل سير العمل أو العمليات الحالية.

يوفر برنامج Segura® PAM مجموعة واسعة من الميزات لتعزيز أمن البنية التحتية الحيوية

سيجورا® بام الانتشار خيارات

لتلبية الاحتياجات المتنوعة للمؤسسات المسؤولة عن البنية التحتية الحيوية، تقدم Segura® PAM خيارات نشر مرنة، بما في ذلك عمليات النشر المحلية والسحابية والهجينة.

يتيح ذلك للمؤسسات اختيار طريقة النشر التي تتوافق بشكل أفضل مع بنيتها التحتية ومتطلباتها الأمنية وقيود ميزانيتها.

ف[illegible]التالي، سنستكشف كيف تحمي Segura® PAM البنية التحتية الحيوية من خلال الخو[illegible] ميزاتها وقدراتها المختلفة بمزيد من التفصيل.







الفصل الخامس

كيف سيجورا®
نظام الحماية PAM
شديد الأهمية
بنية تحتية

منع غير مصرح به وصول

يتمثل أحد الأهداف الرئيسية لبرنامج Segura® PAM في منع الوصول غير المصرح به إلى الأنظمة الحيوية والمعلومات الحساسة. ويتحقق ذلك من خلال عدة ميزات رئيسية، منها:

• التحكم في الوصول القائم على الأدوار (RBAC): يسمح نظام RBAC

تُمكّن Segura® PAM المؤسسات من تحديد وتطبيق ضوابط وصول دقيقة بناءً على أدوار ومسؤوليات المستخدمين ذوي الصلاحيات. ومن خلال ضمان وصول المستخدمين فقط إلى الأنظمة والموارد التي يحتاجونها لأداء مهامهم، تُقلل PAM Segura® من احتمالية تعرضها للهجمات من قِبل الجهات الخبيثة.

• الوصول في الوقت المناسب (JIT) يضمن الوصول في الوقت المناسب ما يلي:

لا تُمنح صلاحيات الوصول المميزة إلا عند الحاجة إليها، وتُسحب فور انتفاء الحاجة إليها. وهذا يقلل من مخاطر الوصول غير المصرح به عن طريق الحد من فرص استغلال المهاجمين لصلاحيات الوصول المميزة.

• إدارة بيانات الاعتماد الآمنة: يوفر Segura® PAM

الإدارة المركزية لبيانات الاعتماد المميزة، بما في ذلك التخزين الآمن والتدوير التلقائي والتدقيق الدوري.

يساعد هذا في منع سرقة بيانات الاعتماد وإساءة استخدامها من خلال ضمان أن تكون بيانات الاعتماد المميزة محدثة دائمًا ومحمية من الوصول غير المصرح به.

الكشف و الرد على التهديدات

صُمم نظام Segura® PAM لمساعدة المؤسسات على اكتشاف الحوادث الأمنية المحتملة والاستجابة لها بسرعة، وذلك من خلال توفير إمكانيات المراقبة والتنبيه في الوقت الفعلي. تشمل الميزات الرئيسية في هذا المجال ما يلي:

مراقبة وتسجيل الجلسات

من خلال مراقبة وتسجيل جلسات المستخدمين ذوي الصلاحيات في الوقت الفعلي، يوفر نظام Segura® PAM رؤية شاملة لأنشطة المستخدمين ذوي الصلاحيات في جميع أنحاء المؤسسة. وهذا يمكّن فرق الأمن من اكتشاف السلوك المشبوه بسرعة واتخاذ الإجراءات المناسبة للتخفيف من المخاطر المحتملة.

الكشف المتقدم عن التهديدات

يدمج نظام Segura® PAM تقنيات التعلم الآلي وتحليلات السلوك لتحديد الحالات الشاذة والتهديدات الأمنية المحتملة بناءً على سلوك المستخدمين وأنماط الوصول السابقة. وهذا يُمكّن المؤسسات من اكتشاف الهجمات المحتملة في مراحلها المبكرة والاستجابة لها قبل أن تتسبب في أضرار جسيمة.

الكشف السريع عن الحوادث الأمنية المحتملة والاستجابة لها من خلال المراقبة في الوقت الفعلي

الالتزام بمعايير ولوائح الصناعة

بالإضافة إلى ميزات الأمان، يساعد نظام Segura® PAM المؤسسات على الالتزام بمعايير ولوائح الصناعة ذات الصلة، مثل HIPAA. وGDPR وNERC CIP ويتحقق ذلك من خلال إمكانيات التدقيق وإعداد التقارير الشاملة، التي تُمكّن المؤسسات من:

• تتبع وتحليل أنشطة الوصول المميز عبر بيئات تكنولوجيا المعلومات والتشغيل الخاصة بهم.

• تحديد انتهاكات الامتثال المحتملة أو المجالات التي تثير القلق.

• إعداد التقارير والأدلة لإثبات الامتثال للمدققين والجهات التنظيمية.



التكامل مع الأنظمة الحالية

بنية تحتية

وأخيرًا، صُمم نظام Segura® PAM ليتكامل بسلاسة مع أنظمة تكنولوجيا المعلومات والتشغيل الحالية، مما يُسهّل على المؤسسات تطبيق وإدارة سياسات الوصول المتميز دون تعطيل سير العمليات أو الإجراءات الحالية. ويشمل ذلك التكامل مع:

أدوات إدارة خدمات [illegible] (ITSM).

[illegible] (SIEM).

من خلال توفير حل شامل ومتكامل لإدارة والتحكم في الوصول المتميز، يمكّن Segura® PAM المؤسسات من حماية أصول البنية التحتية الحيوية والحفاظ على وضع أمني قوي في مواجهة التهديدات والتحديات المتطورة.

في الفصل التالي، سنستكشف دراسات حالة واقعية توضح Segura® PAM أثناء العمل، وتبرز فعاليتها في حماية بيئات البنية التحتية الحيوية.



الفصل السادس

العالم الحقيقي دراسات حالة:

سيجورا® بام قيد الاستخدام

دراسات حالة واقعية توضح فعالية سيجورا®



دراسة حالة ٢
قطاع النقل

واجهت هيئة النقل الوطنية المسؤولة عن إدارة شبكة واسعة من الطرق السريعة والسكك الحديدية والموانئ تحديًا يتمثل في تأمين بنيتها التحتية الحيوية من التهديدات الخارجية والداخلية على حد سواء. لذا، احتاجت الهيئة إلى حل لإدارة الوصول المتميز (PAM)يوفر إدارة آمنة لبيانات الاعتماد، وقدرات كشف التهديدات، والتكامل مع بنيتها التحتية الأمنية الحالية.

بفضل نظام Segura® PAM، تمكنت وكالة النقل من:

• حماية بيانات الاعتماد المميزة من السرقة وسوء الاستخدام من خلال التخزين الآمن والتدوير التلقائي.

• اكتشاف التهديدات الأمنية المحتملة من خلال الاستفادة من التعلم الآلي وتحليلات السلوك لتحديد الحالات الشاذة في سلوك المستخدم.

• التكامل مع أدوات الأمان الحالية، مثل منصات SIEMوأجهزة الشبكة، لتعزيز الوضع الأمني العام.

• الحفاظ على الامتثال للوائح الصناعية ذات الصلة من خلال ميزات التدقيق وإعداد التقارير القوية.



دراسة حالة 1
قطاع الطاقة

واجهت شركة طاقة كبيرة تعمل في عدة دول تحديات في إدارة الوصول المميز إلى بنيتها التحتية المعقدة لتكنولوجيا المعلومات والتشغيل.

كانت الشركة بحاجة إلى حل يوفر تحكمًا دقيقًا في الوصول، ومراقبة في الوقت الفعلي، والامتثال للوائح الصناعية مثل NERC CIP.

من خلال تطبيق نظام Segura® PAM، تمكنت الشركة من:

• تبسيط إدارة الوصول المتميز من خلال توحيد بيانات الاعتماد وسياسات الوصول في منصة مركزية.

• تعزيز الأمن من خلال تطبيق نظام التحكم في الوصول القائم على الأدوار ومنح الوصول في الوقت المناسب للمستخدمين ذوي الامتيازات.

• تحسين الشفافية في الأنشطة ذات الامتيازات من خلال مراقبة وتسجيل جلسات المستخدمين في الوقت الفعلي.

• تحقيق الامتثال لمعايير NERC CIP تلبية المتطلبات من خلال قدرات التدقيق وإعداد التقارير الشاملة.



دراسة حالة 3
مرفق المياه

واجهت إحدى شركات المياه الكبرى، المسؤولة عن توفير مياه الشرب النظيفة وخدمات معالجة مياه الصرف الصحي لملايين العملاء، تحديًا يتمثل في تأمين بنيتها التحتية الحيوية من الهجمات الإلكترونية والتهديدات الداخلية. لذا، احتاجت الشركة إلى حل لإدارة الوصول المتميز (PAM) يوفر تحكمًا دقيقًا في الوصول، ومراقبة الجلسات، وإدارة بيانات الاعتماد بشكل آمن.

من خلال تطبيق نظام Segura® PAM، حققت شركة المياه ما يلي:

- تعزيز الأمن من خلال تطبيق التحكم في الوصول القائم على الأدوار والوصول في الوقت المناسب للمستخدمين المتميزين.
- تحسين الرؤية للأنشطة ذات الامتيازات من خلال مراقبة وتسجيل الجلسات في الوقت الفعلي.
- إدارة آمنة للصلاحيات بيانات الاعتماد، بما في ذلك كلمات المرور والمفاتيح والشهادات.
- الامتثال للوائح الخاصة بالصناعة، مثل برنامج إدارة المخاطر التابع لوكالة حماية البيئة (RMP).

توضح دراسات الحالة هذه فعالية Segura® PAM في حماية البنية التحتية الحيوية عبر مختلف القطاعات وتسلط الضوء على فوائد تطبيق حل PAM شامل.



في الفصل التالي، سنناقش كيف يمكن للمؤسسات تطبيق Segura® PAM في بيئاتها الخاصة والخطوات اللازمة لضمان نجاح عملية النشر.



الفصل السابع

التنفيذ سيجورا® بام في مؤسستكم

يُعدّ نشر حل شامل لإدارة الوصول المتميز (PAM) مثل Segura® PAM خطوةً حاسمةً في تعزيز أمان بنيتك التحتية الحيوية. في هذا الفصل، سنوضح الخطوات الرئيسية لتنفيذ .Segura®

إدارة الوصول المتميز (PAM) في مؤسستك وتقديم التوجيهات لضمان النشر الناجح.

تقييم وضعك الحالي
الوضع الأمني

قبل تطبيق Segura® PAM، من الضروري تقييم الوضع الأمني الحالي لمؤسستك. يشمل ذلك تحديد الثغرات الأمنية الموجودة، وتقييم مدى امتثال مؤسستك للوائح الخاصة بالقطاع، وتحديد مدى فعالية سياسات وإجراءات إدارة الوصول المتميز الحالية. سيساعدك هذا التقييم على تحديد المجالات التي تحتاج فيها Segura® إلى تحسين.

يمكن أن يوفر نظام إدارة الأداء (PAM) تحسينات كبيرة ويرشد استراتيجية التنفيذ الخاصة بك.

تحديد الأدوار وسياسات الوصول

تتمثل إحدى الوظائف الأساسية لبرنامج Segura® PAM في تطبيق ضوابط وصول دقيقة بناءً على أدوار ومسؤوليات المستخدمين ذوي الصلاحيات. ولتحقيق ذلك، ستحتاج إلى تحديد الأدوار وسياسات الوصول المناسبة لمؤسستك.

وهذا يشمل:

• تحديد أدوار المستخدمين ذوي الامتيازات المختلفة داخل مؤسستك.

• تحديد مستويات الوصول والأذونات المطلوبة لـ كل دور.

• وضع سياسات الوصول، مثل الوصول في الوقت المناسب والرفع المؤقت للامتيازات، لتقليل مخاطر الوصول غير المصرح به.

نشر سيجورا® بام

بناءً على المتطلبات والبنية التحتية الخاصة بمؤسستك، يمكنك اختيار نشر Segura® PAM محليًا، أو في السحابة، أو باستخدام نهج هجين.

بغض النظر عن خيار النشر الذي تختاره، فإن عملية التنفيذ ستتضمن عمومًا الخطوات التالية:

• تثبيت وتكوين برنامج Segura® PAM على الخادم المناسب أو بيئة السحابة.

• دمج Segura® PAM مع أنظمة تكنولوجيا المعلومات والتشغيل الحالية لديك الأنظمة، مثل حلول إدارة الهوية والوصول (IAM)، ومنصات إدارة معلومات الأمان والأحداث (SIEM)، وأجهزة الشبكة.

• تهيئة Segura® PAM لفرض الأدوار المحددة لديك وسياسات الوصول.

• استيراد أو إنشاء بيانات اعتماد مميزة داخل منصة Segura® PAM.

التدريب و
وعي

يتطلب تطبيق نظام إدارة الوصول المتميز (PAM) بنجاح ليس فقط التكنولوجيا المناسبة، بل أيضاً التدريب والتوعية اللازمين بين موظفيك. تأكد من تدريب جميع المستخدمين ذوي الصلاحيات في مؤسستك على الاستخدام الأمثل لنظام Segura® PAM، بما في ذلك:

- تسجيل الدخول والمصادقة من خلال Segura® PAM منصة.
- طلب واستخدام الوصول المميز، وفقًا للسياسات المعمول بها.
- التعرف على الحوادث الأمنية المحتملة والإبلاغ عنها تم اكتشافها من خلال ميزات مراقبة الجلسات والكشف عن التهديدات.

بالإضافة إلى ذلك، من الضروري رفع مستوى الوعي بين المستخدمين غير المتميزين بشأن أهمية إدارة الوصول المتميز والدور الذي تلعبه في تأمين البنية التحتية الحيوية لمؤسستك.



مستمر
الصيانة والمراقبة

يُعدّ تطبيق Segura® PAMمجرد بداية رحلتك نحو بنية تحتية حيوية أكثر أمانًا. يُعدّ الصيانة والمراقبة المنتظمة ضروريين لضمان استمرار فعالية حلّ PAMالخاص بك. ويشمل ذلك ما يلي:

- مراجعة وتحديث الأدوار وسياسات الوصول بشكل دوري لتعكس التغييرات داخل مؤسستك.

- مراقبة جلسات المستخدمين ذوي الامتيازات والاستجابة للحوادث الأمنية المحتملة في الوقت الفعلي.

- التدقيق وإعداد التقارير عن أنشطة الوصول المميز للحفاظ على الامتثال للوائح الخاصة بالصناعة.

باتباع هذه الخطوات وأفضل الممارسات، يمكن لمؤسستك تنفيذ Segura® PAMبنجاح وتعزيز أمان أصول البنية التحتية الحيوية الخاصة بك.

في الفصل التالي، سنختتم مناقشتنا ونقدم إرشادات حول الخطوات التالية للمؤسسات التي تتطلع إلى نشر PAM. Segura®





الخاتمة والخطوات التالية

لقد استكشفنا في هذا الكتاب الإلكتروني أهمية أمن البنية التحتية الحيوية، ودور إدارة الوصول المميز (PAM)في حماية الأصول الحيوية، وفوائد تطبيق حل PAMشامل مثل .Segura® PAM

عند التفكير في تطبيق Segura® PAMداخل مؤسستك، ضع الخطوات التالية في الاعتبار:

1 قم بتقييم الوضع الأمني الحالي لمؤسستك، بما في ذلك نقاط الضعف الحالية، والامتثال للوائح الخاصة بالصناعة، وفعالية سياسات وإجراءات إدارة الوصول المميز الحالية.

2 حدد الأدوار المناسبة وسياسات الوصول لمنظمتك، مع ضمان أن المستخدمين ذوي الامتيازات لا يمكنهم الوصول إلا إلى الأنظمة والموارد التي يحتاجونها لأداء واجباتهم.

3 اختر خيار النشر المناسب لـ - Segura® PAMسواء كان محليًا أو قائمًا على السحابة أو هجينًا -بناءً على البنية التحتية لمؤسستك ومتطلبات الأمان وقيود الميزانية.

4 قم بتدريب المستخدمين ذوي الامتيازات على الاستخدام الصحيح لـ Segura® PAMوقم برفع مستوى الوعي بين المستخدمين غير ذوي الامتيازات بشأن أهمية إدارة الوصول المتميز في تأمين البنية التحتية الحيوية.

5 قم بمراقبة وصيانة نشر Segura® PAMالخاص بك، بما في ذلك مراجعة وتحديث الأدوار وسياسات الوصول بشكل دوري، ومراقبة جلسات المستخدمين ذوي الامتيازات، والتدقيق والإبلاغ عن أنشطة الوصول ذات الامتيازات.



باتباع هذه الخطوات، يمكن لمؤسستك نشر Segura® PAMبنجاح وتعزيز وضعها الأمني للبنية التحتية الحيوية.

مع استمرار تطور مشهد التهديدات، سيكون تطبيق حل شامل لإدارة الوصول المتميز مثل Segura® PAMأمرًا ضروريًا لحماية أصولك الحيوية، وضمان سلامة ورفاهية عملائك، والحفاظ على استقرار عالمنا المترابط.

هل أنت مستعد لتجربة مباشرة كيف يمكن لـ Segura® PAMأن يعزز أمن البنية التحتية الحيوية لمؤسستك؟

ندعوكم لحجز عرض توضيحي مُخصّص مع فريق خبرائنا، الذين سيُعرّفونكم على الميزات والقدرات الرئيسية لبرنامج Segura PAM، ويُوضّحون لكم كيف يُمكنه مساعدتكم في إدارة والتحكم في الوصول المُميّز بكفاءة. خلال العرض التوضيحي، يُمكنكم توقع ما يلي:

• اكتساب فهم أعمق لحل Segura PAMوكيف يعالج التحديات الفريدة لتأمين البنية التحتية الحيوية.

• استكشف واجهة المستخدم سهلة الاستخدام والميزات القوية لـ Segura PAM، بما في ذلك التحكم الدقيق في الوصول، وإدارة بيانات الاعتماد الآمنة، ومراقبة الجلسات في الوقت الفعلي، والكشف المتقدم عن التهديدات.

• ناقش متطلبات الأمان والبنية التحتية الخاصة بمؤسستك، وتعرف على كيفية تخصيص ونشر Segura PAM لتلبية احتياجاتك.

• الحصول على فرصة لطرح الأسئلة وتلقيها
إرشادات شخصية من فريق خبراء إدارة الأصول الشخصية لدينا.

لحجز عرض توضيحي، ما عليك سوى النقر هنا وملء نموذج الطلب بمعلومات الاتصال الخاصة بك والتاريخ والوقت المفضلين لديك. بمجرد إرسال طلبك، سيتواصل معك أحد أعضاء فريقنا لتأكيد التفاصيل وتزويدك بالتعليمات اللازمة للانضمام إلى العرض التوضيحي.

لا تفوّت هذه الفرصة لاكتشاف كيف يمكن لـ Segura PAMمساعدة مؤسستك في حماية أصول بنيتها التحتية الحيوية، والامتثال للوائح الخاصة بالقطاع، ومواكبة التهديدات الأمنية المتطورة. احجز عرضك التوضيحي اليوم!

هل أنت مستعد لرفع مستوى الأمن السيبراني لمؤسستك؟

اكتشف حلول ®Segura المتطورة لحماية البيانات الحساسة والأنظمة الحيوية من التهديدات الإلكترونية.

اطلب عرضًا تجريبيًا الآن

سيجورا®: أمن الهوية المستقبلي.

تُعدّ ®Segura رائدةً في مجال إدارة الوصول المتميز (PAM)، حيث تُقدّم حلول أمان سريعة وبسيطة وفعّالة، دون أي تعقيدات. منصتنا سهلة الاستخدام وقابلة للتطوير تُبسّط إدارة الوصول المتميز، وهي مُصممة خصيصًا لفرق تكنولوجيا المعلومات التي تتعامل مع سيناريوهات واقعية يوميًا.

تحظى ®Segura بتقدير عالمي من قبل KuppingerCole وGartner وFrost & Sullivan لابتكارها وموثوقيتها وتجربة عملائها الاستثنائية. وعلى منصة Gartner Peer Insights، يصنف المستخدمون الحقيقيون حلنا باستمرار كأفضل نظام لإدارة الوصول المتميز (PAM).

أمان قوي، لا إضاعة للوقت - هذا هو سيجورا®.

segura | Futureproof Identity Security | segura.security



كتاب إلكتروني

الحماية
شديد الأهمية
بنية تحتية

EBOOK

SHIELDING CRITICAL INFRASTRUCTURE





Introduction

The Imperative to Secure Critical Infrastructure in Today's Digital Landscape

In today's interconnected world, critical infrastructure serves as the backbone of our society, enabling essential services such as energy, transportation, healthcare, and communication. However, securing these vital systems has become increasingly challenging as cyber threats continue to evolve and grow in sophistication. With the European Union Agency for Cybersecurity (ENISA) stating that 30% of all cyberattacks targeted critical infrastructure sectors in 2019, the need for robust security measures has never been more urgent.

The consequences of security breaches in critical infrastructure can be devastating. Organizations face significant financial losses, with the Ponemon Institute estimating the average cost of a data breach for critical infrastructure organizations at $4.29 million. Additionally, disruptions to essential services can have far-reaching social and economic impacts. 85% of the United States' critical infrastructure is owned and operated by the private sector.

The American Society of Civil Engineers (ASCE) 2021 Infrastructure Report Card highlights the need for significant investment in improving and securing the nation's critical infrastructure, giving the United States a C- grade. As the International Energy Agency (IEA) estimates that global investments in energy infrastructure must reach $3.5 trillion annually through 2050 to meet global climate and energy goals, the importance of securing these investments becomes even more critical.

In this ebook, we will explore the importance of critical infrastructure, the various threats and challenges it faces, and the role of Privileged Access Management (PAM) in ensuring its security. We will also introduce the Segura® PAM solution and demonstrate how it can effectively protect critical infrastructure systems in a rapidly evolving digital landscape.

By understanding the risks and implementing robust security measures, organizations can safeguard their critical infrastructures and ensure the continued delivery of essential services for years to come.

Table of Contents

Chapter 1

Introduction to Critical Infrastructure and Its Importance

Defining Critical Infrastructure

As the world becomes more interdependent, securing and maintaining the stability of critical infrastructure has become indispensable for the smooth functioning of society and the economy. Critical infrastructure encompasses the assets, systems, and networks, both physical and virtual, that are crucial to a nation's operations. This includes sectors such as energy, water, transportation, communications, and emergency services, among others.

The disruption or devastation of these vital infrastructures can lead to severe consequences, affecting not only the specific sectors but also public safety, national security, and the overall economy. Consequently, prioritizing the security and resilience of critical infrastructure has emerged as a primary concern for governments and organizations across the globe.

> The stability of critical infrastructure has become indispensable for the smooth functioning of society and the economy.

The Importance of Critical Infrastructure

Critical infrastructure forms the backbone of modern society, providing essential services that affect every aspect of daily life. The importance of critical infrastructure cannot be overstated, as it ensures the smooth functioning of various sectors.

The failure or disruption of any of these critical infrastructures could lead to widespread consequences, including the loss of life, economic damage, and the erosion of public trust. As such, safeguarding critical infrastructure is paramount to maintaining national security, public safety, and economic stability.

Energy

The generation, transmission, and distribution of electricity, natural gas, and other forms of energy that power our homes, businesses, and industries.

Water

The supply of clean and safe drinking water, as well as the treatment and disposal of wastewater.

Transportation

The movement of people and goods by air, land, and sea, including highways, railways, ports, and airports.

Communications

The transmission of information through various mediums, such as the internet, telephone networks, and satellite systems.

Emergency services

The provision of medical, police, and fire services that protect the health and safety of citizens.

The Growing Need for Critical Infrastructure Protection

As the world becomes more interconnected and reliant on technology, the potential for cyber-attacks on critical infrastructure has grown exponentially. Cybercriminals, nation-states, and other malicious actors are increasingly targeting critical infrastructure, seeking to exploit vulnerabilities and gain unauthorized access to sensitive information, control systems, or other vital assets.

The risks associated with cyber threats to critical infrastructure are further exacerbated by factors such as:

- The increased use of digital technologies and the convergence of information technology (IT) and operational technology (OT) systems, which create new vulnerabilities and attack surfaces.
- The growing reliance on third-party vendors and supply chain partners, which can introduce additional risks and complexities.
- The rapid pace of technological change, which can make it challenging for organizations to keep up with evolving threats and maintain a robust security posture.

Given these challenges, it is more important than ever for organizations to implement comprehensive security measures to protect their critical infrastructure and ensure its continued resilience.

The Role of Privileged Access Management in Critical Infrastructure Protection

One of the key components of critical infrastructure protection is the effective management and control of privileged access. Privileged access refers to the elevated permissions granted to specific users, allowing them to perform sensitive tasks, access critical systems, or manage security controls.

Privileged access management (PAM) is a crucial aspect of critical infrastructure security, as it helps organizations prevent unauthorized access, detect and respond to threats, and maintain compliance with relevant industry standards and regulations. PAM solutions, such as the Segura® PAM, provide the necessary tools and capabilities to manage, monitor, and control privileged access, thereby reducing the risk of security breaches and protecting critical infrastructure from potential attacks.

In the following chapters, we will delve deeper into the threats and challenges to critical infrastructure security, the role of privileged access management in addressing these challenges, and how the Segura® PAM solution can help organizations protect their critical infrastructure assets.



Chapter 2

Threats and Challenges to Critical Infrastructure Security

Understanding the Threat Landscape

The security of critical infrastructure is under constant threat from a wide range of actors, including nation-states, cybercriminals, hacktivists, and even insiders. These malicious actors employ a variety of tactics, techniques, and procedures (TTPs) to compromise critical infrastructure systems, disrupt services, or cause physical damage. Some of the most common threats to critical infrastructure security include:

Cyberattacks

Cybercriminals and nation-state actors target critical infrastructure systems using various types of malware, ransomware, and distributed denial of service (DDoS) attacks to disrupt operations, steal sensitive information, or cause physical damage.

Supply chain attacks

Third-party vendors or suppliers can introduce vulnerabilities into critical infrastructure systems, either through compromised hardware or software, or by providing unauthorized access to threat actors.

Insider threats

Employees, contractors, or other insiders with privileged access can intentionally or unintentionally compromise critical infrastructure systems, either through malicious actions or negligence.

Physical attacks

Critical infrastructure assets can also be targeted by physical threats, such as terrorism, sabotage, or natural disasters, which can cause significant damage or disruption to operations.

Challenges in Securing Critical Infrastructure

Protecting critical infrastructure from the myriad threats outlined above is a complex task, compounded by several unique challenges, including:

- **Convergence of IT and OT:** The integration of information technology (IT) and operational technology (OT) systems has increased efficiency and connectivity but has also introduced new vulnerabilities that can be exploited by cybercriminals.
- **Legacy systems:** Many critical infrastructure sectors rely on outdated systems that were not designed with modern security threats in mind, making them more susceptible to attacks.
- **Inadequate visibility and monitoring:** The sheer scale and complexity of critical infrastructure systems make it difficult for organizations to maintain complete visibility and monitoring of their networks, devices, and access points.
- **Regulatory compliance:** Organizations responsible for critical infrastructure must comply with various industry-specific regulations and standards, which can be complex and time-consuming to manage.
- **Limited resources:** Many critical infrastructure organizations face budget constraints, staffing shortages, or a lack of in-house expertise, making it challenging to implement and maintain robust security measures.

The Critical Role of Privileged Access Management

Given the threats and challenges associated with critical infrastructure security, it is essential for organizations to implement a comprehensive Privileged Access Management (PAM) solution, such as Segura® PAM. PAM is a critical component of a robust security posture, as it helps organizations:

Prevent unauthorized access

By controlling and managing privileged access, organizations can reduce the risk of unauthorized access to critical systems, whether from external attackers or insiders.

Detect and respond to threats

PAM solutions can provide real-time monitoring and alerting of suspicious activities, enabling organizations to quickly detect and respond to potential security incidents.

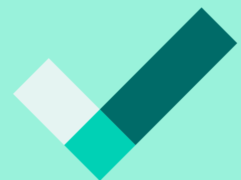
Maintain regulatory compliance

PAM solutions can help organizations meet the requirements of various industry-specific regulations and standards, such as NERC CIP, GDPR, and HIPAA, by ensuring proper access controls, auditing, and reporting capabilities.

Improve visibility and control

A comprehensive PAM solution provides organizations with the visibility and control needed to manage privileged access across their IT and OT environments, reducing the risk of security breaches.

In the next chapter, we will explore the role of Privileged Access Management in more detail, including its key components and how it can help organizations protect their critical infrastructure assets.



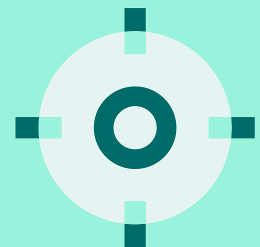
Chapter 3

Understanding the Role of Privileged Access Management (PAM)

The Importance of Privileged Access Management

As discussed in the previous chapters, the security of critical infrastructure is heavily dependent on the effective management and control of privileged access. Privileged users, such as system administrators, IT personnel, and third-party vendors, have elevated permissions that grant them access to critical systems and sensitive information. If not properly managed, this access could be exploited by malicious actors, leading to significant security breaches and potential damage to critical infrastructure.

Privileged Access Management (PAM) is a crucial component of a robust security strategy, helping organizations prevent unauthorized access, detect and respond to threats, and maintain compliance with industry-specific regulations.



Key Components of PAM

A comprehensive PAM solution, such as Segura® PAM, typically includes the following key components:

- **Access Control:** PAM solutions provide granular access controls, allowing organizations to define and enforce who can access which systems, under what conditions, and for how long. This includes features such as role-based access control (RBAC), just-in-time (JIT) access, and temporary elevation of privileges.

- **Credential Management:** PAM solutions offer centralized management of privileged credentials, including passwords, keys, and certificates. This includes capabilities such as secure storage, automatic rotation, and periodic auditing of credentials.

- **Session Monitoring and Recording:** PAM solutions enable organizations to monitor and record privileged user sessions in real-time, providing complete visibility and accountability for privileged activities. This helps organizations detect suspicious activity and facilitates forensic investigations in the event of a security incident.

- **Auditing and Reporting:** PAM solutions provide comprehensive auditing and reporting capabilities, allowing organizations to track and analyze privileged access activities and demonstrate compliance with industry-specific regulations and standards.

- **Threat Detection and Response:** Advanced PAM solutions incorporate machine learning and behavioral analytics to identify anomalies and potential security threats, enabling organizations to quickly detect and respond to incidents before they escalate.

Benefits of Implementing PAM in Critical Infrastructure Security

Implementing a robust PAM solution, such as Segura® PAM, offers numerous benefits for organizations responsible for critical infrastructure, including:

Enhanced Security

By managing and controlling privileged access, organizations can significantly reduce the risk of unauthorized access and security breaches, protecting both their critical systems and sensitive information.

Improved Compliance

PAM solutions help organizations demonstrate compliance with various industry-specific regulations and standards by providing the necessary access controls, auditing, and reporting capabilities.

Greater Operational Efficiency

By automating and streamlining privileged access processes, PAM solutions can improve operational efficiency and reduce the risk of human error.

Increased Visibility and Control

PAM solutions provide organizations with the visibility and control needed to effectively manage privileged access across their IT and OT environments, ensuring that privileged access is granted only to those who truly need it.



In the following chapters, we will explore Segura® PAM in more detail, including its key features, how it protects critical infrastructure, and real-world case studies demonstrating its effectiveness in action.



Chapter 4

Segura® PAM: An Overview and Key Features

Introduction to Segura® PAM

Segura® Privileged Access Management (PAM) is a comprehensive solution designed to help organizations protect their critical infrastructure by managing and controlling privileged access across their IT and OT environments.

Segura® PAM provides a robust set of features and capabilities that enable organizations to prevent unauthorized access, detect and respond to threats, and maintain compliance with relevant industry standards and regulations.

Key Features of Segura® PAM

Segura® PAM offers a wide range of features that make it an ideal solution for organizations looking to enhance their critical infrastructure security. Some of the key features of Segura® PAM include:

- **Granular Access Control:** Segura® PAM provides role-based access control (RBAC) and just-in-time (JIT) access, ensuring that privileged users only have access to the systems they need when they need it. This helps to minimize the risk of unauthorized access and security breaches.
- **Secure Credential Management:** Segura® PAM offers centralized management of privileged credentials, including passwords, keys, and certificates. This includes secure

storage, automatic rotation, and periodic auditing of credentials to ensure their integrity and reduce the risk of compromise.

- **Session Monitoring and Recording:** Segura® PAM enables organizations to monitor and record privileged user sessions in real-time, providing complete visibility and accountability for privileged activities. This helps to detect suspicious activity and facilitates forensic investigations in the event of a security incident.
- **Advanced Threat Detection and Response:** Segura® PAM incorporates machine learning and behavioral analytics to identify anomalies and potential security threats, enabling organizations to quickly detect and respond to incidents before they escalate.
- **Comprehensive Auditing and Reporting:** Segura® PAM provides extensive auditing and reporting capabilities, allowing organizations to track and analyze privileged access activities and demonstrate compliance with industry-specific regulations and standards.
- **Integration with Existing Infrastructure:** Segura® PAM seamlessly integrates with existing IT and OT systems, making it easy for organizations to implement and manage their privileged access policies without disrupting existing workflows or processes.

Segura® PAM offers a wide range of features to enhance critical infrastructure security

Segura® PAM Deployment Options

To cater to the diverse needs of organizations responsible for critical infrastructure, Segura® PAM offers flexible deployment options, including on-premises, cloud-based, and hybrid deployments.

This allows organizations to choose the deployment method that best aligns with their infrastructure, security requirements, and budget constraints.

In the next chapter, we will explore how Segura® PAM protects critical infrastructure by delving into its various features and capabilities in greater detail.







Chapter 5

How Segura® PAM Protects Critical Infrastructure

Preventing Unauthorized Access

One of the primary goals of Segura® PAM is to prevent unauthorized access to critical systems and sensitive information. This is achieved through several key features, including:

- **Role-Based Access Control (RBAC):** RBAC allows organizations to define and enforce granular access controls based on the roles and responsibilities of privileged users. By ensuring that users only have access to the systems and resources they need to perform their duties, Segura® PAM minimizes the potential attack surface for malicious actors.
- **Just-In-Time (JIT) Access:** JIT access ensures that privileged access is granted only when it is required and revoked as soon as it is no longer needed. This reduces the risk of unauthorized access by limiting the window of opportunity for attackers to exploit privileged credentials.
- **Secure Credential Management:** Segura® PAM provides centralized management of privileged credentials, including secure storage, automatic rotation, and periodic auditing. This helps to prevent credential theft and misuse by ensuring that privileged credentials are always up-to-date and protected from unauthorized access.

Detecting and Responding to Threats

Segura® PAM is designed to help organizations quickly detect and respond to potential security incidents by providing real-time monitoring and alerting capabilities. Key features in this area include:

Session Monitoring and Recording

By monitoring and recording privileged user sessions in real-time, Segura® PAM provides complete visibility into privileged activities across the organization. This enables security teams to quickly detect suspicious behavior and take appropriate action to mitigate potential threats.

Advanced Threat Detection

Segura® PAM incorporates machine learning and behavioral analytics to identify anomalies and potential security threats based on historical user behavior and access patterns. This allows organizations to detect potential attacks in their early stages and respond before they can cause significant damage.

> Quickly detect and respond to potential security incidents by real-time monitoring

Maintaining Compliance with Industry Standards and Regulations

In addition to its security features, Segura® PAM also helps organizations maintain compliance with relevant industry standards and regulations, such as NERC CIP, GDPR, and HIPAA. This is achieved through comprehensive auditing and reporting capabilities, which enable organizations to:

- Track and analyze privileged access activities across their IT and OT environments.
- Identify potential compliance violations or areas of concern.
- Generate reports and evidence to demonstrate compliance to auditors and regulators.



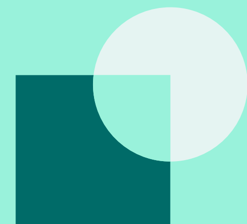
Integrating with Existing Infrastructure

Finally, Segura® PAM is designed to integrate seamlessly with existing IT and OT systems, making it easy for organizations to implement and manage their privileged access policies without disrupting existing workflows or processes. This includes integration with:

- Identity and access management (IAM) solutions.
- Security information and event management (SIEM) platforms.
- IT service management (ITSM) tools.
- Network and security devices.

By providing a comprehensive, integrated solution for managing and controlling privileged access, Segura® PAM enables organizations to protect their critical infrastructure assets and maintain a robust security posture in the face of evolving threats and challenges.

In the next chapter, we will explore real-world case studies that demonstrate Segura® PAM in action, showcasing its effectiveness in protecting critical infrastructure environments.





Chapter 6

Real-world Case Studies: Segura® PAM in Action

Real-world case studies that demonstrate the effectiveness of Segura®



Case Study 1
Energy Sector

A large energy company with operations across multiple countries faced challenges in managing privileged access to its complex IT and OT infrastructure. The company needed a solution that would provide granular access control, real-time monitoring, and compliance with industry regulations such as NERC CIP.

By implementing Segura® PAM, the company was able to:

- Streamline privileged access management by consolidating credentials and access policies in a centralized platform.
- Enhance security by enforcing role-based access control and just-in-time access for privileged users.
- Improve visibility into privileged activities by monitoring and recording user sessions in real-time.
- Achieve compliance with NERC CIP requirements through comprehensive auditing and reporting capabilities.



Case Study 2
Transportation Sector

A national transportation agency responsible for managing a vast network of highways, railways, and ports faced the challenge of securing its critical infrastructure from both external and internal threats. The agency needed a PAM solution that would provide secure credential management, threat detection capabilities, and integration with its existing security infrastructure.

With Segura® PAM, the transportation agency was able to:

- Protect privileged credentials from theft and misuse through secure storage and automatic rotation.
- Detect potential security threats by leveraging machine learning and behavioral analytics to identify anomalies in user behavior.
- Integrate with existing security tools, such as SIEM platforms and network devices, to enhance overall security posture.
- Maintain compliance with relevant industry regulations through robust auditing and reporting features.



Case Study 3
Water Utility

A large water utility responsible for providing clean drinking water and wastewater treatment services to millions of customers faced the challenge of securing its critical infrastructure from cyber-attacks and insider threats. The utility required a PAM solution that would provide granular access control, session monitoring, and secure credential management.

By deploying Segura® PAM, the water utility achieved:

- Enhanced security by implementing role-based access control and just-in-time access for privileged users.
- Improved visibility into privileged activities through real-time session monitoring and recording.
- Secure management of privileged credentials, including passwords, keys, and certificates.
- Compliance with industry-specific regulations, such as the EPA's Risk Management Program (RMP).

These case studies demonstrate the effectiveness of Segura® PAM in protecting critical infrastructure across various sectors and highlight the benefits of implementing a comprehensive PAM solution.



In the next chapter, we will discuss how organizations can implement Segura® PAM in their own environments and the steps to ensure a successful deployment.



Chapter 7

Implementing Segura® PAM in Your Organization

Deploying a comprehensive Privileged Access Management (PAM) solution like Segura® PAM is a critical step in enhancing the security of your critical infrastructure. In this chapter, we will outline the key steps involved in implementing Segura® PAM in your organization and provide guidance on ensuring a successful deployment.

Assessing Your Current Security Posture

Before implementing Segura® PAM, it is essential to assess your organization's current security posture. This involves identifying existing vulnerabilities, evaluating your organization's compliance with industry-specific regulations, and determining the effectiveness of your current privileged access management policies and procedures. This assessment will help you identify areas where Segura® PAM can provide the most significant improvements and guide your implementation strategy.

Defining Roles and Access Policies

One of the primary functions of Segura® PAM is to enforce granular access controls based on the roles and responsibilities of privileged users. To achieve this, you will need to define the appropriate roles and access policies for your organization.

This involves:

- Identifying the various privileged user roles within your organization.
- Mapping the required access levels and permissions for each role.
- Establishing access policies, such as just-in-time access and temporary elevation of privileges, to minimize the risk of unauthorized access.

Deploying Segura® PAM

Depending on your organization's specific requirements and infrastructure, you can choose to deploy Segura® PAM on-premises, in the cloud, or using a hybrid approach. Regardless of the deployment option you choose, the implementation process will generally involve the following steps:

- Installing and configuring the Segura® PAM software on the appropriate server(s) or cloud environment.
- Integrating Segura® PAM with your existing IT and OT systems, such as identity and access management (IAM) solutions, security information and event management (SIEM) platforms, and network devices.
- Configuring Segura® PAM to enforce your defined roles and access policies.
- Importing or creating privileged credentials within the Segura® PAM platform.

Training and Awareness

A successful PAM implementation requires not only the right technology but also the proper training and awareness among your staff. Ensure that all privileged users within your organization are trained on the proper use of Segura® PAM, including:

- Logging in and authenticating through the Segura® PAM platform.
- Requesting and using privileged access, in accordance with established policies.
- Recognizing and reporting potential security incidents detected through session monitoring and threat detection features.

Additionally, it's essential to raise awareness among non-privileged users regarding the importance of privileged access management and the role it plays in securing your organization's critical infrastructure.



Ongoing Maintenance and Monitoring

Implementing Segura® PAM is just the beginning of your journey toward a more secure critical infrastructure. Regular maintenance and monitoring are necessary to ensure the ongoing effectiveness of your PAM solution. This includes:

- Periodically reviewing and updating roles and access policies to reflect changes within your organization.
- Monitoring privileged user sessions and responding to potential security incidents in real-time.
- Auditing and reporting on privileged access activities to maintain compliance with industry-specific regulations.

By following these steps and best practices, your organization can successfully implement Segura® PAM and enhance the security of your critical infrastructure assets.

In the next chapter, we will conclude our discussion and provide guidance on the next steps for organizations looking to deploy Segura® PAM.



Conclusion and Next Steps

Throughout this ebook, we have explored the importance of critical infrastructure security, the role of Privileged Access Management (PAM) in protecting critical assets, and the benefits of implementing a comprehensive PAM solution like Segura® PAM.

As you consider implementing Segura® PAM within your organization, keep the following next steps in mind:

1. Assess your organization's current security posture, including existing vulnerabilities, compliance with industry-specific regulations, and the effectiveness of your current privileged access management policies and procedures.
2. Define the appropriate roles and access policies for your organization, ensuring that privileged users only have access to the systems and resources they need to perform their duties.
3. Choose the appropriate deployment option for Segura® PAM (on--premises, cloud-based, or hybrid) based on your organization's infrastructure, security requirements, and budget constraints.
4. Train privileged users on the proper use of Segura® PAM and raise awareness among non-privileged users regarding the importance of privileged access management in securing critical infrastructure.
5. Monitor and maintain your Segura® PAM deployment, including periodically reviewing and updating roles and access policies, monitoring privileged user sessions, and auditing and reporting on privileged access activities.



By following these steps, your organization can successfully deploy Segura® PAM and strengthen its critical infrastructure security posture.

As the threat landscape continues to evolve, implementing a comprehensive PAM solution like Segura® PAM will be essential in safeguarding your critical assets, ensuring the safety and well-being of your customers, and maintaining the stability of our interconnected world.

Are you ready to experience firsthand how Segura® PAM can enhance your organization's critical infrastructure security?

We invite you to schedule a personalized demo with our team of experts, who will guide you through the key features and capabilities of Segura PAM and demonstrate how it can help you manage and control privileged access effectively. During the demo, you can expect to:

- Gain a deeper understanding of the Segura PAM solution and how it addresses the unique challenges of securing critical infrastructure.
- Explore the user-friendly interface and powerful features of Segura PAM, including granular access control, secure credential management, real-time session monitoring, and advanced threat detection.
- Discuss your organization's specific security requirements and infrastructure, and learn how Segura PAM can be customized and deployed to meet your needs.
- Have the opportunity to ask questions and receive personalized guidance from our team of PAM experts.

To schedule your demo, simply **click here** and fill out the request form with your contact information and preferred date and time. Once your request is submitted, a member of our team will be in touch to confirm the details and provide you with the necessary instructions to join the demo.

Don't miss this opportunity to discover how Segura PAM can help your organization protect its critical infrastructure assets, maintain compliance with industry-specific regulations, and stay ahead of evolving security threats. Schedule your demo today!

Ready to elevate your organization's cybersecurity?

Discover Segura®'s cutting-edge solutions to protect sensitive data and critical systems from cyber threats.

REQUEST A DEMO NOW

Segura®: Futureproof Identity Security.

Segura® is a leader in Privileged Access Management (PAM), delivering security that's fast, simple, and powerful—without the complexity. Our intuitive, scalable platform simplifies privileged access management, designed for real IT teams dealing with real-world scenarios every day.

Segura® is globally recognized by Gartner, KuppingerCole, and Frost & Sullivan for innovation, reliability, and exceptional customer experience. On Gartner Peer Insights, real users consistently rank our solution as the #1 PAM.

> Powerful security,
> zero time wasted—
> that's Segura®.



EBOOK

SHIELDING CRITICAL INFRASTRUCTURE

Document Classification: Public | April 2025